

Mikrochip mit einem diesen ganz oder teilweise umgebenden lichtundurchlässigen Ummantelungsabschnitt

Patent number: DE19601390
Publication date: 1997-07-17
Inventor: GRUBER MARTIN (DE)
Applicant: SIEMENS AG (DE)
Classification:
- **international:** H04L9/10; H04L12/22; H01L23/552; H01L23/06; G06K19/073
- **european:** G06K19/073, H01L23/58B
Application number: DE19961001390 19960116
Priority number(s): DE19961001390 19960116

Also published as:

WO9726727 (A3)

WO9726727 (A2)

Abstract of DE19601390

The microchip described is characterized in that a light-sensitive element is fitted at a point which light can reach only if the sheathing or parts of it are removed and/or destroyed by use not in accordance with the design specifications.

Data supplied from the **esp@cenet** database - Worldwide

THIS PAGE BLANK (USPTO)



①⑨ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑫ Patentschrift
⑩ DE 196 01 390 C 2

⑳ Aktenzeichen: 196 01 390.9-31
㉑ Anmeldetag: 16. 1. 96
㉒ Offenlegungstag: 17. 7. 97
㉓ Veröffentlichungstag
der Patenterteilung: 16. 7. 98

㉔ Int. Cl.⁶:
H 04 L 9/10
H 04 L 12/22
H 01 L 23/552
H 01 L 23/06
G 06 K 19/073
G 06 F 11/00

DE 196 01 390 C 2

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

㉕ Patentinhaber:
Siemens AG, 80333 München, DE

㉖ Erfinder:
Gruber, Martin, 92421 Schwandorf, DE

㉗ Für die Beurteilung der Patentfähigkeit in Betracht
gezogene Druckschriften:

US 52 33 563
US 51 59 629
US 50 53 992

DE-Z: BETIRAC, Michael et al.: Mehr Sicherheit
für Prozessorkarten. In: Funkschau, 1991, H. 20,
S. 76-78;

㉘ Mikrochip

㉙ Mikrochip mit einem lichtempfindlichen Element, wo-
bei im Ansprechen auf einen Lichteinfall auf das lichtemp-
findliche Element sofort oder später eine Reaktion erfolgt,
deren Art und Umfang von einer vorherigen Aktivierung
abhängt und ein zumindest teilweises Löschen von ge-
speicherter Information und/oder eine Zerstörung des Mi-
krochips oder Teilen desselben umfaßt.

DE 196 01 390 C 2

Beschreibung

Die vorliegende Erfindung betrifft einen Mikrochip mit einem lichtempfindlichen Element, wobei im Ansprechen auf einen Lichteinfall auf das lichtempfindliche Element sofort oder später eine Reaktion erfolgt, die ein zumindest teilweises Löschen von gespeicherter Information und/oder eine Zerstörung des Mikrochips oder Teilen desselben umfaßt.

Derartige Mikrochips sind beispielsweise aus der US 5 053 992, der US 5 159 629, der US 5 233 563, und dem Aufsatz "Mehr Sicherheit in Prozessorkarten" von Betirac Michel et al. in der Zeitschrift Funkschau, 1991, Heft 20, Seiten 76 bis 78 bekannt.

Die lichtempfindlichen Elemente sind dabei Bestandteile von Schutzmechanismen, die den Mikrochip vor elektrischen und/oder optischen Analysen schützen sollen. Sie sind an Stellen vorgesehen, an welche nur bei Entfernung und/oder Zerstörung einer den Mikrochip ganz oder teilweise umgebenden Ummantelung oder Teilen derselben Licht gelangen kann, und veranlassen bei Lichteinfall ein zumindest teilweises Löschen von im Mikrochip gespeicherter Information oder eine Zerstörung des Mikrochips oder Teilen desselben.

Die wie erwähnt angeordneten und verwendeten lichtempfindlichen Elemente schützen den Chip relativ gut vor Ausspähungsversuchen. Sie erschweren andererseits die Herstellung und das Testen der Mikrochips, denn auch hierbei darf ja kein Licht auf die lichtempfindlichen Elemente gelangen. Das Vorsehen von lichtempfindlichen Elementen der erwähnten Art im Mikrochip ist daher mit einem nicht unerheblichen Zusatzaufwand verbunden, was erkennbar ein Nachteil ist.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, einen Mikrochip zu schaffen, bei dem auf einfache Weise und mit minimalem Aufwand zuverlässig verhindert werden kann, daß er durch Unberechtigte analysiert wird.

Diese Aufgabe wird erfindungsgemäß im wesentlichen dadurch gelöst, daß die im Ansprechen auf einen Lichteinfall auf das lichtempfindliche Element erfolgende Reaktion der Art und dem Umfang nach von einer vorherigen Aktivierung abhängt und wenigstens ein zumindest teilweises Löschen von gespeicherter Information und/oder eine Zerstörung des Mikrochips oder Teilen desselben umfaßt.

Da der Schutzmechanismus, dessen Bestandteil das lichtempfindliche Element ist, erst durch eine gesonderte Aktivierung in Betrieb genommen wird, können die Herstellung und das Testen des Mikrochips bei noch nicht aktiviertem oder deaktiviertem Schutzmechanismus erfolgen.

Bei dem erfindungsgemäßen Mikrochip ist damit auf einfache Weise und mit minimalem Aufwand zuverlässig verhindert, daß er durch Unberechtigte analysiert wird.

Vorteilhafte Weiterbildungen der Erfindung sind Gegenstand der Unteransprüche.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels näher erläutert.

Ausgangspunkt ist ein vor einer unbefugten Fremdanalyse zu schützender, beispielsweise (aber nicht ausschließlich) in einer Chipkarte enthaltener Mikrochip. Der Mikrochip kann ein beliebiges elektronisches Element sein; in der Regel wird es sich hierbei jedoch um eine integrierte Schaltung wie einen Mikroprozessor, Signalprozessor, Mikrocontroller, Speicherbaustein oder dergleichen handeln.

Der Mikrochip ist ganz oder teilweise von einem lichtundurchlässigen Ummantelungsabschnitt (im folgenden der Einfachheit halber kurz als Ummantelung bezeichnet) umgeben, um ihn mechanisch zu schützen und um eine optische Analyse von dessen Aufbau und Strukturen zu verhin-

dern.

Die lichtundurchlässige Ummantelung bedeckt zumindest die sicherheitsrelevanten Bereich des Mikrochips.

5 Sofern auch eine elektrische Analyse des Mikrochips ausgeschlossen sein soll, sind auch die elektrischen Anschlußstellen des Mikrochips und die mit diesen verbundenen Signalleitungen, gegebenenfalls auch eine äußere Beschaltung des zu schützenden Mikrochips von der Ummantelung umgeben.

10 Die Ummantelung kann durch ein Gehäuse, ein gehäuseartiges Gebilde (beispielsweise Vergußmassen bzw. sogenannte Globe-Top-Abdeckungen bei in Chipkarten enthaltenen Mikrochips und dergleichen) oder ein Teil derselben gebildet werden; alternativ oder ergänzend kann sie auch durch ein über dem zu schützenden Mikrochip angeordnetes weiteres elektrisches, elektromechanisches oder mechanisches Bauelement, beispielsweise durch einen auf den zu schützenden Mikrochip direkt oder indirekt (d. h. unter Einfügung einer Isolationsschicht oder dergleichen) aufgesetzten zweiten Mikrochip, oder ein Teil desselben gebildet werden.

Erfindungsgemäß sind nun innerhalb des Mikrochip-Ummantelungsgebildes ein oder mehrere lichtempfindliche Elemente vorgesehen.

25 Die lichtempfindlichen Elemente können dabei in die Ummantelung integriert sein und/oder an der Oberfläche und/oder im Inneren des Mikrochips vorgesehen sein. Sie sind vorzugsweise über oder in unmittelbarer Nähe von denjenigen Stellen des Mikrochips angeordnet, dessen ungehinderte Freilegung für eine Analyse des Mikrochips förderlich sein könnte.

Bei bestimmungsgemäßem Umgang mit dem wie beschrieben ummantelten Mikrochip fällt auf das lichtempfindliche Element aufgrund der Lichtundurchlässigkeit der darüber liegenden Ummantelung nie Licht. Bei bestimmungsfremdem Umgang mit dem Mikrochip, d. h. bei Freilegen desselben unter Entfernen und/oder Zerstören der Ummantelung oder spätestens beim Versuch einer unter Beleuchtung durchzuführenden optischen Analyse oder einem ebenfalls unter Beleuchtung durchzuführenden Anschließen von Signalleitungen zum Auslesen von Speichereinhalten oder dergleichen trifft hingegen zwangsläufig Licht auf das lichtempfindliche Element.

45 Dies löst in Abhängigkeit von der Art des lichtempfindlichen Elements unterschiedliche Vorgänge im lichtempfindlichen Element aus.

Ist das lichtempfindliche Element ein Speicherelement, dessen Inhalt beim Einfall von Licht veränderbar ist, kann dieser Speichereinhalt durch eine hierzu vorgesehene Steuerungseinrichtung (Sicherheitslogik) ausgewertet werden. Das Auslesen des Speicherelements und die Auswertung des Inhalts kann dabei zu beliebigen Anlässen (beispielsweise immer bei Anlegen einer Betriebsspannung) und/oder Zeitpunkten erfolgen. Wird dabei festgestellt, daß ein Lichteinfall auf das lichtempfindliche Element stattgefunden hat, also ein Versuch unternommen wird, den Mikrochip zu analysieren, wird dies zum Anlaß genommen, eine vom Typ des lichtempfindlichen Elements unabhängige, später noch genauer beschriebene Reaktion zu veranlassen.

60 Ist das lichtempfindliche Element ein fotoelektrisches Wandlerelement, das bei Lichteinfall eine Spannung erzeugt, kann diese Spannung dazu verwendet werden, eine vom Typ des lichtempfindlichen Elements unabhängige, später noch genauer beschriebene Reaktion zu veranlassen bzw. durchzuführen.

Ist das lichtempfindliche Element ein bei Lichteinfall seine elektrischen Eigenschaften veränderndes Element, können die veränderten elektrischen Eigenschaften zur Rea-

lisierung einer Schaltfunktion verwendet werden, mittels welcher eine vom Typ des lichtempfindlichen Elements unabhängige, später noch genauer beschriebene Reaktion veranlaßbar bzw. durchführbar ist.

Die Reaktion auf das Erfassen eines Lichteinfalls bzw. auf einen Lichteinfall besteht allgemein gesprochen darin, daß Maßnahmen getroffen werden, die eine Analyse des zu schützenden Mikroprozessors unmöglich machen. Die Reaktion kann beispielsweise darin bestehen, daß gespeicherte Informationen ganz oder teilweise gelöscht und/oder der Mikrochip oder einzelner Funktionen desselben zerstört werden (beispielsweise durch Zünden sogenannter Fuses). Darüber hinaus können auf das Erfassen eines Lichteinfalls hin bzw. auf einen Lichteinfall hin selbstverständlich auch beliebige andere Reaktionen ausgelöst werden, die die Analyse des zu schützenden Chips erschweren oder ausschließen.

Um zu verhindern, daß ein Lichteinfall auf das lichtempfindliche Element schon bei der Herstellung des Mikrochips die beschriebene Reaktion zeigt, ist gegebenenfalls ein Aktivierungsprozeß vorzusehen, durch welchen die ursprünglich noch nicht aktivierten Reaktionen aktivierbar sind, beispielsweise indem eine Sicherheitslogik irreversibel von einem Aus-Zustand in einen Bereitschaftszustand versetzt wird.

Die spektrale Empfindlichkeit des lichtempfindlichen Elements ist vorzugsweise so ausgelegt, daß nicht nur der Einfall von sichtbarem Licht, sondern auch der Einfall anderer Strahlungsarten, die zur Sichtbarmachung von Mikrochip-Strukturen verwendbar sind, durch das lichtempfindliche Element erfäßbar sind. Sofern das gesamte Strahlungsspektrum nicht durch ein einzelnes lichtempfindliches Element abgedeckt werden kann, kann in Betracht gezogen werden, jeweils mehrere lichtempfindliche Elemente vorzusehen, die sich diesbezüglich ergänzen.

Die über einem lichtempfindlichen Element vorgesehene Chip-Ummantelung ist vorzugsweise so ausgebildet, daß sie für sämtliche Strahlungs-Wellenlängen, die durch das lichtempfindliche Element erfäßbar ist, undurchlässig ist; sofern bestimmte Strahlungswellenlängen in der Umgebung des zu schützenden Chips üblicherweise nicht vorkommen, kann es sich als vorteilhaft erweisen, die Ummantelung hierfür durchlässig zu gestalten.

Patentansprüche

1. Mikrochip mit einem lichtempfindlichen Element, wobei im Ansprechen auf einen Lichteinfall auf das lichtempfindliche Element sofort oder später eine Reaktion erfolgt, deren Art und Umfang von einer vorherigen Aktivierung abhängt und ein zumindest teilweises Löschen von gespeicherter Information und/oder eine Zerstörung des Mikrochips oder Teilen desselben umfaßt.

2. Mikrochip nach Anspruch 1, dadurch gekennzeichnet, daß das lichtempfindliche Element an einer Stelle vorgesehen ist, an welche nur unter bestimmungsfremder Entfernung und/oder Zerstörung eines den Mikrochip ganz oder teilweise umgebenden lichtundurchlässigen Ummantelungsabschnittes oder Teilen desselben Licht gelangen kann.

3. Mikrochip nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Mikrochip Bestandteil einer Chipkarte ist.

4. Mikrochip nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Ummantelungsabschnitt durch ein gehäuseartiges Gebilde oder ein Teil desselben gebildet wird.

5. Mikrochip nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der Ummantelungsabschnitt durch ein über dem Mikrochip angeordnetes weiteres Bauelement oder ein Teil desselben gebildet wird.

6. Mikrochip nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das lichtempfindliche Element ein auf einen Lichteinfall ansprechendes Speicherelement ist.

7. Mikrochip nach Anspruch 6, dadurch gekennzeichnet, daß eine Sicherheitslogik vorgesehen ist, welche die im Speicherelement gespeicherte Information zu gegebenen Anlässen und/oder zu gegebenen Zeitpunkten ausliest, auswertet und entsprechend darauf reagiert.

8. Mikrochip nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das lichtempfindliche Element ein fotoelektrisches Wandlerelement ist, welches bei Lichteinfall eine Spannung erzeugt.

9. Mikrochip nach Anspruch 8, dadurch gekennzeichnet, daß die erzeugte Spannung zum zumindest teilweisen Löschen von gespeicherter Information und/oder zum Zerstören des Mikrochips oder Teilen desselben verwendet wird.

10. Mikrochip nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das lichtempfindliche Element ein bei Lichteinfall seine elektrischen Eigenschaften veränderndes Element ist.

11. Mikrochip nach Anspruch 10, dadurch gekennzeichnet, daß die veränderten elektrischen Eigenschaften zur Realisierung einer Schaltfunktion verwendet werden, mittels welcher eine ein zumindest teilweises Löschen von gespeicherter Information und/oder ein Zerstören des Mikrochips oder Teilen desselben veranlassende Spannung durchschaltbar ist.

- Leerseite -